[RENESAS SECURITY PROCESS INTRODUCTION TRAINING]

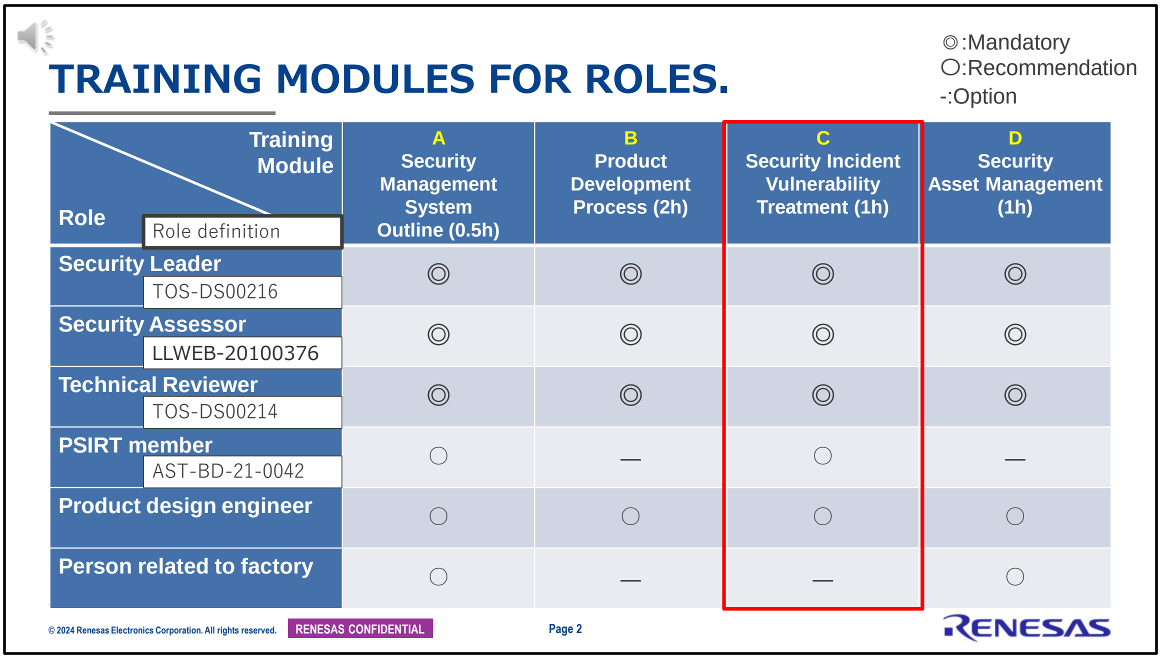
PROCESS TO ADDRESS SECURITY INCIDENTS AND VULNERABILITIES.

(RCT-JF3009)

REV.3.0 3RD.JUN. 2024 REL/QA/QAD/QSP/QDSC S. NAGATA, K. FUJII

RENESAS CONFIDENTIAL

I will explain the process to address security incidents and vulnerabilities.



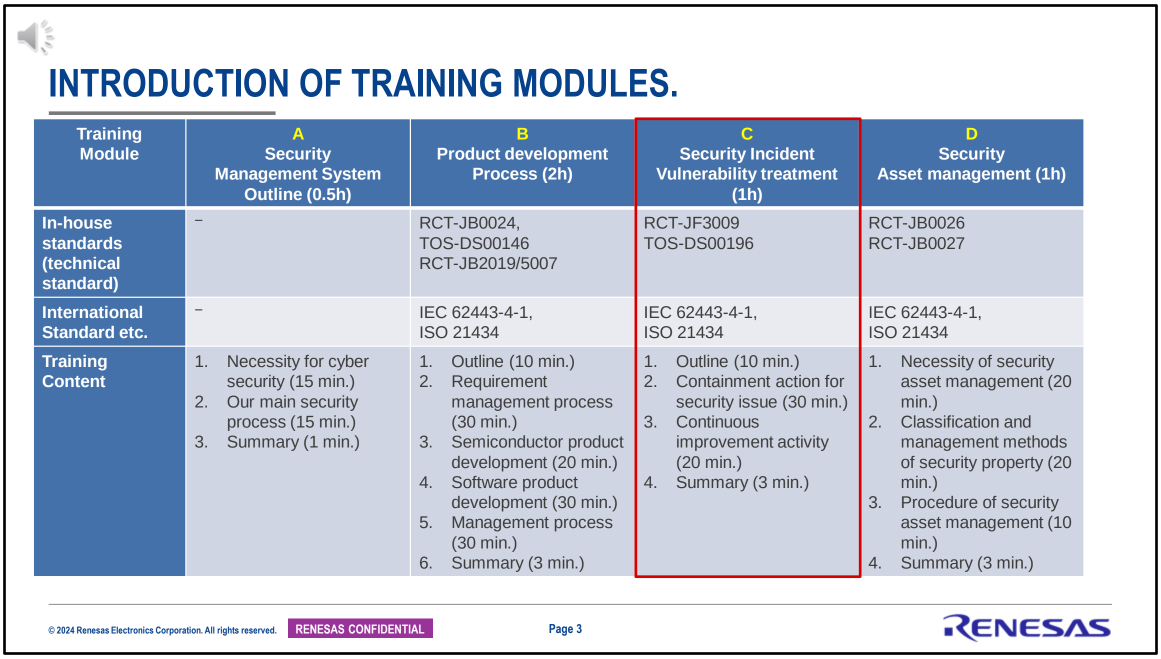
TRAINING MODULES FOR ROLES.

◎:Mandatory
〇:Recommendation
-:Option

Training Module Role	Role definition	A Security Management System Outline (0.5h)	B Product Development Process (2h)	C Security Incident Vulnerability Treatment (1h)	D Security Asset Management (1h)
Security Leader	TOS-DS00216	◎	◎	◎	◎
Security Assessor	LLWEB-20100376	◎	◎	◎	◎
Technical Reviewer	TOS-DS00214	◎	◎	◎	◎
PSIRT member	AST-BD-21-0042	○	—	○	—
Product design engineer		○	○	○	○
Person related to factory		○	—	—	○

RENESAS CONFIDENTIAL Page 2

First, I would like to explain the position of this course. There is a certification system for each security-related role. The certification system is stipulated in the role standards shown in the square on the left. Required education has been designated for this purpose, and one of the required education is this process basic education. This table shows the degree of necessity for each security role in process basic education modules A, B, C, and D. Those with double circles are required to attend, and those with single circles are optional. These are disclosed on the Design Quality Portal page, and anyone can take them at their leisure and obtain the evidence for your role certification by passing the comprehension test in the portal page. This course corresponds to the third C course among these basic process courses. Regarding role certification, the system differs between HPCSG and EPSG, so please refer to each group web site for details.

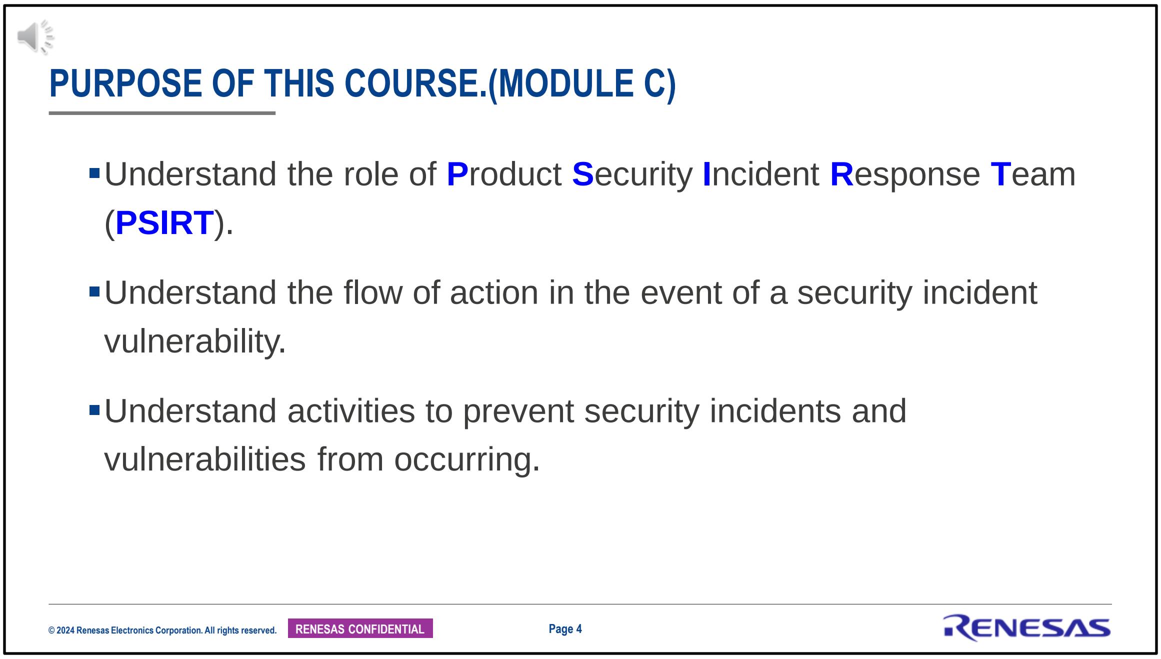


INTRODUCTION OF TRAINING MODULES.

Training Module	A Security Management System Outline (0.5h)	B Product development Process (2h)	C Security Incident Vulnerability treatment (1h)	D Security Asset management (1h)
In-house standards (technical standard)	–	RCT-JB0024, TOS-DS00146 RCT-JB2019/5007	RCT-JF3009 TOS-DS00196	RCT-JB0026 RCT-JB0027
International Standard etc.	–	IEC 62443-4-1, ISO 21434	IEC 62443-4-1, ISO 21434	IEC 62443-4-1, ISO 21434
Training Content	1. Necessity for cyber security (15 min.) 2. Our main security process (15 min.) 3. Summary (1 min.)	1. Outline (10 min.) 2. Requirement management process (30 min.) 3. Semiconductor product development (20 min.) 4. Software product development (30 min.) 5. Management process (30 min.) 6. Summary (3 min.)	1. Outline (10 min.) 2. Containment action for security issue (30 min.) 3. Continuous improvement activity (20 min.) 4. Summary (3 min.)	1. Necessity of security asset management (20 min.) 2. Classification and management methods of security property (20 min.) 3. Procedure of security asset management (10 min.) 4. Summary (3 min.)

RENESAS CONFIDENTIAL

This is the approximate time required for each education from A to D. The total time is about 4 and a half hour, and this module C is just under 1 hour.

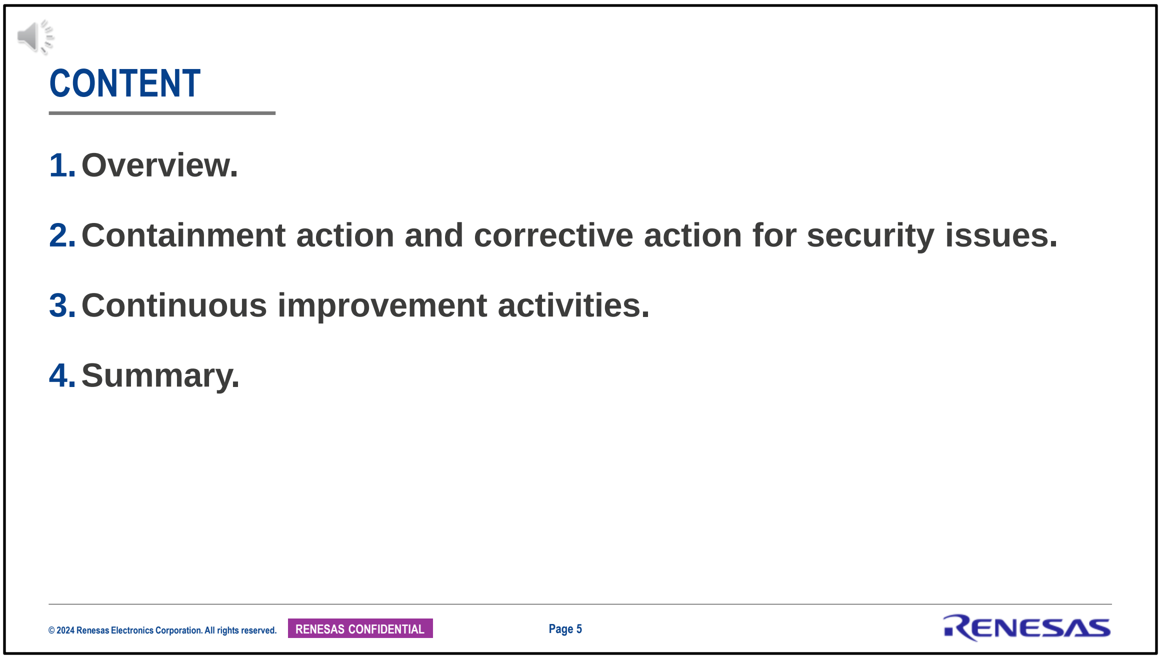


PURPOSE OF THIS COURSE.(MODULE C)

- Understand the role of **P**roduct **S**ecurity **I**ncident **R**esponse **T**eam (**PSIRT**).
- Understand the flow of action in the event of a security incident vulnerability.
- Understand activities to prevent security incidents and vulnerabilities from occurring.

RENESAS CONFIDENTIAL Page 4

The purpose of this course is as you can see here, but as explained on the previous page, It also includes the purpose of security roles certification.



CONTENT

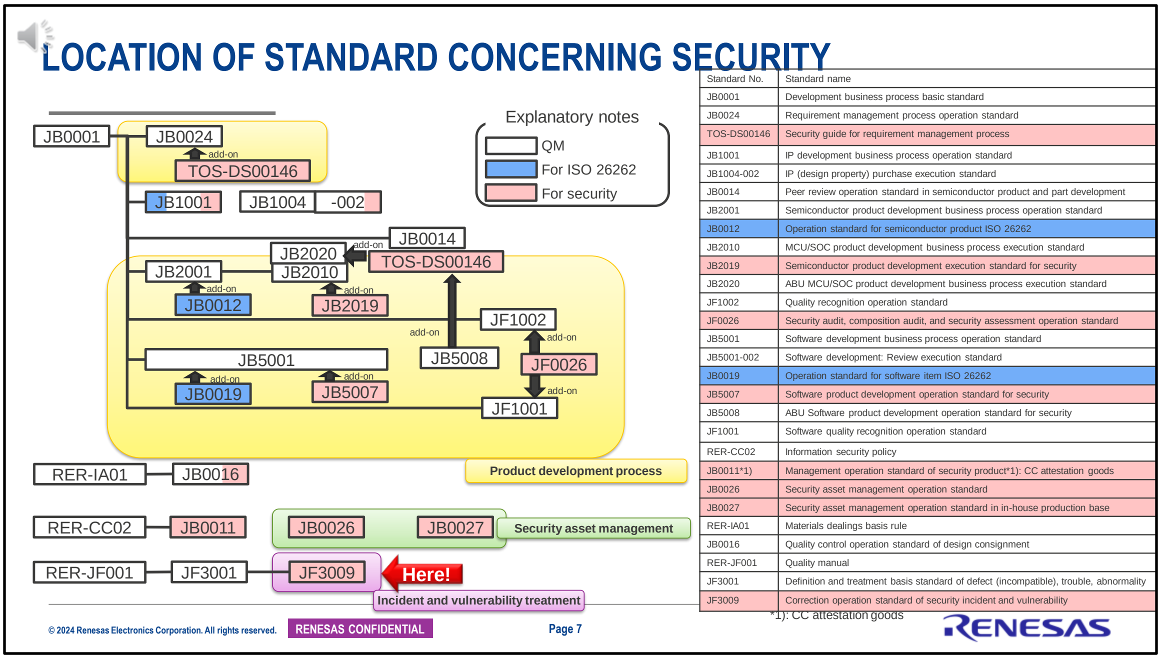
1. Overview.
2. Containment action and corrective action for security issues.
3. Continuous improvement activities.
4. Summary.

RENESAS CONFIDENTIAL

Regarding the content of this course, we have two aspect to be explained, that is, one is the activities to address security issues and another one is the activities to monitor and take countermeasures for vulnerability information continuously, those both are defined in RCT-JB3009.

1. OVERVIEW

Chapter 1. This is overview of this course.



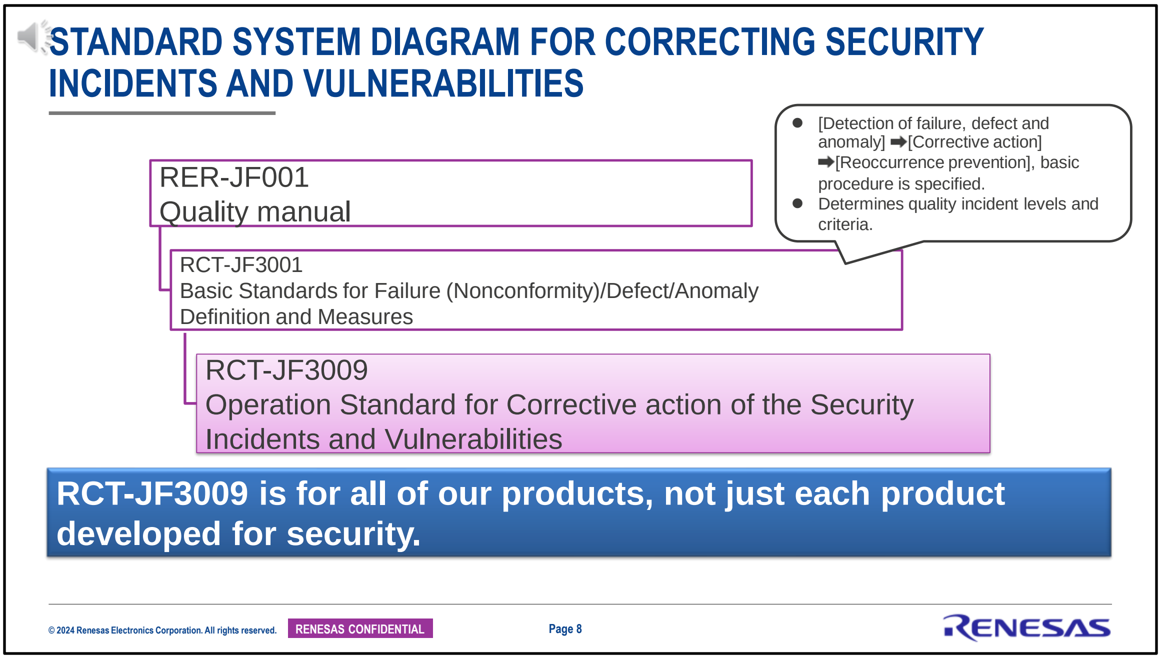
LOCATION OF STANDARD CONCERNING SECURITY

Standard No.	Standard name
JB0001	Development business process basic standard
JB0024	Requirement management process operation standard
TOS-DS00146	Security guide for requirement management process
JB1001	IP development business process operation standard
JB1004-002	IP (design property) purchase execution standard
JB0014	Peer review operation standard in semiconductor product and part development
JB2001	Semiconductor product development business process operation standard
JB0012	Operation standard for semiconductor product ISO 26262
JB2010	MCU/SOC product development business process execution standard
JB2019	Semiconductor product development execution standard for security
JB2020	ABU MCU/SOC product development business process execution standard
JF1002	Quality recognition operation standard
JF0026	Security audit, composition audit, and security assessment operation standard
JB5001	Software development business process operation standard
JB5001-002	Software development: Review execution standard
JB0019	Operation standard for software item ISO 26262
JB5007	Software product development operation standard for security
JB5008	ABU Software product development operation standard for security
JF1001	Software quality recognition operation standard
RER-CC02	Information security policy
JB0011*1)	Management operation standard of security product*1): CC attestation goods
JB0026	Security asset management operation standard
JB0027	Security asset management operation standard in in-house production base
RER-IA01	Materials dealings basis rule
JB0016	Quality control operation standard of design consignment
RER-JF001	Quality manual
JF3001	Definition and treatment basis standard of defect (incompatible), trouble, abnormality
JF3009	Correction operation standard of security incident and vulnerability

*1): CC attestation goods

RENESAS CONFIDENTIAL

This diagram provides an overview of how the process of corrective action for security incidents and vulnerabilities（RCT-JF3009）which will be explained in this course, is positioned within the overall quality system. For your attention, process basic education modules A already explained it to you, so if you have already seen it, you can skip the explanation on this page. First of all, the table on the right is a list of technical standards related to product development. And on the left ,this is a diagram of the interrelationship of technical standards. White squares are QM-related, blue squares are functional safety-related, and red squares security-related standards. Additionally, the scope covered by this basic security process course has been further categorized into three categories. In the system diagram on the left, the yellow category corresponds to modules A and B in the development process, the purple category corresponds to module C of this course, and the green category corresponds to module D. RCT-JF3009 is in JF's 3000 quality control system related to abnormality handling management and independent from the yellow development process and the green security information management process. However, keep in mind that operationally they are closely interconnected.



STANDARD SYSTEM DIAGRAM FOR CORRECTING SECURITY INCIDENTS AND VULNERABILITIES

- [Detection of failure, defect and anomaly] ➡[Corrective action] ➡[Reoccurrence prevention], basic procedure is specified.
- Determines quality incident levels and criteria.

RER-JF001
Quality manual

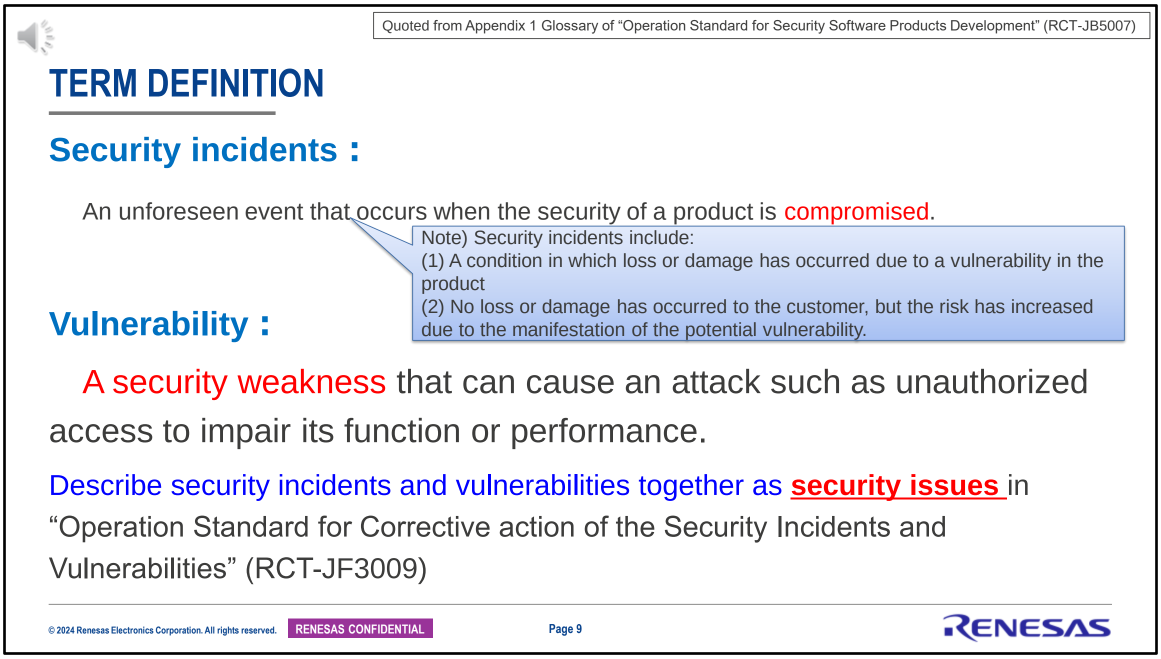
RCT-JF3001
Basic Standards for Failure (Nonconformity)/Defect/Anomaly Definition and Measures

RCT-JF3009
Operation Standard for Corrective action of the Security Incidents and Vulnerabilities

RCT-JF3009 is for all of our products, not just each product developed for security.

RENESAS CONFIDENTIAL Page 8

Next, I would like to add a little more information about the positioning of the JF3000 series that I just explained in previous page. RCT-JF3001, which is the parent of RCT-JF3009, stipulates procedures for identifying the problem and preventing recurrence when an abnormality occurs in a non-security general product. On the other hand, JF3009 includes additional procedures that are required in addition to the general procedures if the product in question is security-related. What you need to understand is that even if a product is from an older era and was developed in a time when security development processes did not exist, if a security problem were to occur, JF3009 would need to be taken in addition to JF3001. On the other hand, even if a product was developed in an era where a security development process existed, JF3001 can be followed as long as there are no security-related defects. I will not explain JF3001 today, but anyone in any role involved in development needs to understand both JF3001 and JF3009.



Quoted from Appendix 1 Glossary of "Operation Standard for Security Software Products Development" (RCT-JB5007)

TERM DEFINITION

Security incidents :

An unforeseen event that occurs when the security of a product is compromised.

Note) Security incidents include:
(1) A condition in which loss or damage has occurred due to a vulnerability in the product
(2) No loss or damage has occurred to the customer, but the risk has increased due to the manifestation of the potential vulnerability.

Vulnerability :

A security weakness that can cause an attack such as unauthorized access to impair its function or performance.

Describe security incidents and vulnerabilities together as **security issues** in "Operation Standard for Corrective action of the Security Incidents and Vulnerabilities" (RCT-JF3009)

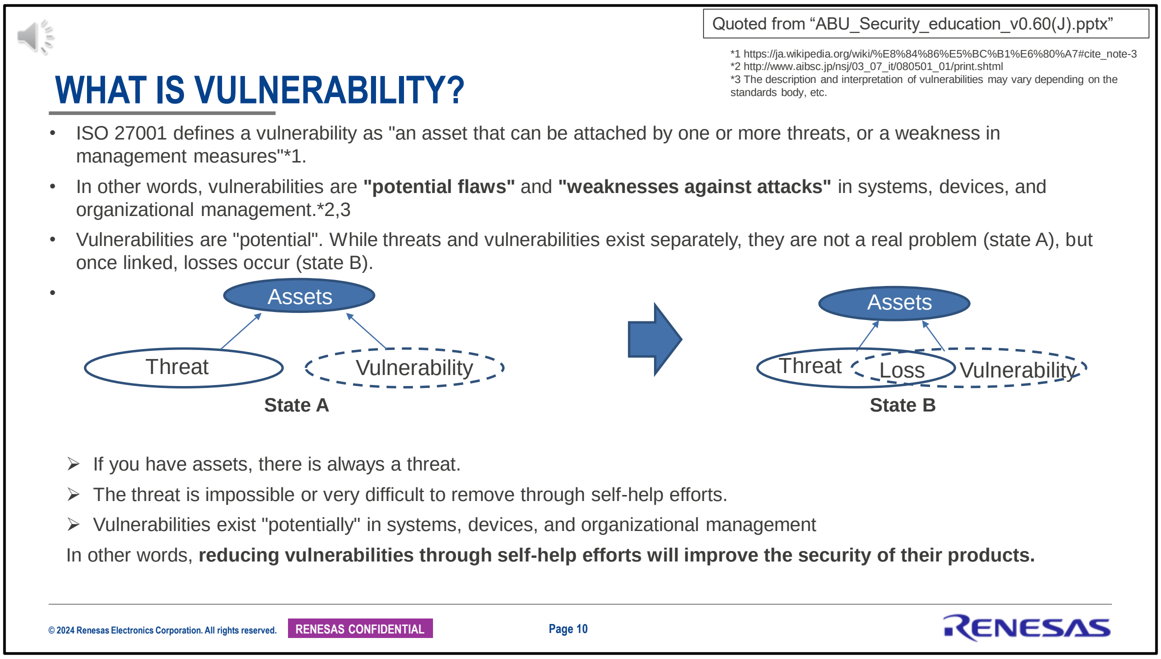
RENESAS CONFIDENTIAL

Page 9

RENESAS

Here we explain definitions of technical terms. What do the words "security incident" and "vulnerability" that appear in the title of this course actually mean? You often hear about it in newspapers and TV, but it is precisely defined by the ISO international standard. However, because it is necessary to change the expressions to be easier to understand for Renesas internal personnel during their daily work, we have provided internal term definitions in the appendix of RCT-JB5007.
First, let me explain the word incident. The RCT-JB5007 appendix defines this as an unexpected situation where security is compromised. The word "compromised" is written in red here, but it is only when security is compromised that it is called an incident. As mentioned in the explanation of the balloon, the term "compromised" refers to cases in which damage actually occurs due to a vulnerability, and cases in which the risk of damage increases even if no damage has occurred yet. In other words, if a vulnerability is discovered but there is no actual damage and the risk is low, it cannot be called a "compromised"yet, so it cannot be called an incident.
Next, let me explain the word vulnerability. In the RCT-JB5007 appendix, it is defined as a security weakness that can cause damage

to functionality or performance due to attacks such as unauthorized access. This is just a term that refers to a state where it is just a weakness and has not yet reached the point of “compromised”. In JF3009, the two words incident and vulnerability are collectively defined as a security issues. When a problem occurs, it is important to pay attention to the distinction between the two terms incident and vulnerability in order to avoid confusion in communication.



Quoted from “ABU_Security_education_v0.60(J).pptx”

WHAT IS VULNERABILITY?

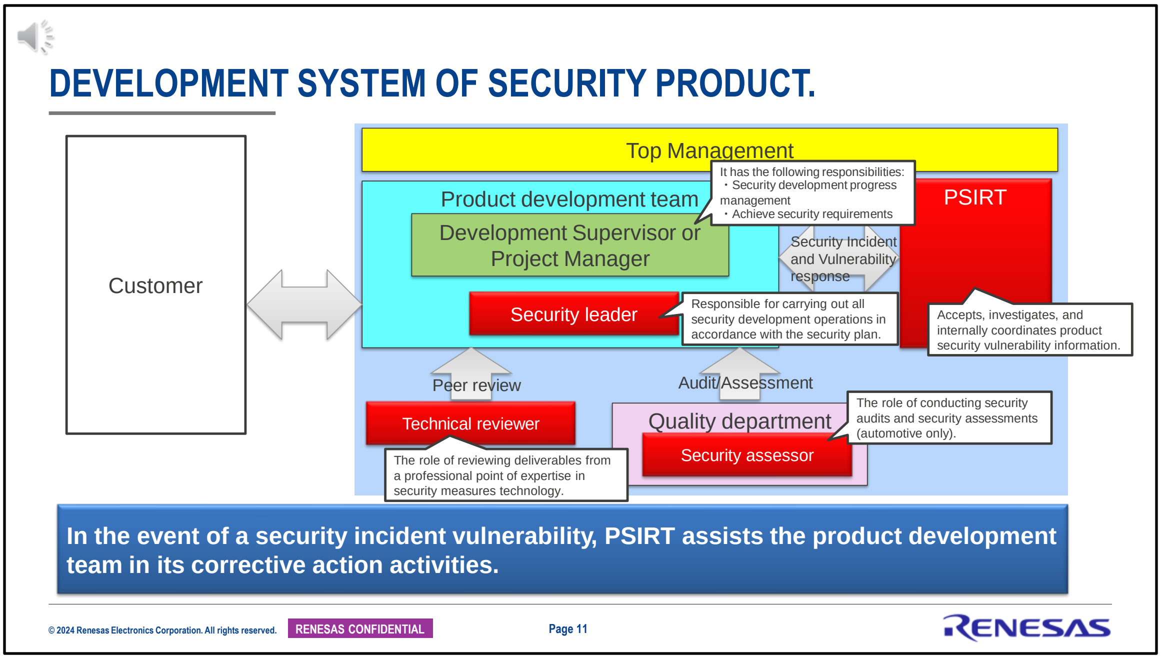
- ISO 27001 defines a vulnerability as "an asset that can be attached by one or more threats, or a weakness in management measures"*1.
- In other words, vulnerabilities are **"potential flaws"** and **"weaknesses against attacks"** in systems, devices, and organizational management.*2,3
- Vulnerabilities are "potential". While threats and vulnerabilities exist separately, they are not a real problem (state A), but once linked, losses occur (state B).
-

- ➢ If you have assets, there is always a threat.
- ➢ The threat is impossible or very difficult to remove through self-help efforts.
- ➢ Vulnerabilities exist "potentially" in systems, devices, and organizational management

In other words, **reducing vulnerabilities through self-help efforts will improve the security of their products.**

*1 https://ja.wikipedia.org/wiki/%E8%84%86%E5%BC%B1%E6%80%A7#cite_note-3
*2 http://www.aibsc.jp/nsj/03_07_it/080501_01/print.shtml
*3 The description and interpretation of vulnerabilities may vary depending on the standards body, etc.

Let me explain a little more about the word vulnerability that I explained in the previous slide. Please pay attention to the difference between state A and state B on the left and right sides of this diagram. As shown in state A, as long as there are security assets, threats and vulnerabilities will remain latent at any time. When these threats and vulnerabilities overlap to reach state B, it becomes apparent as a loss. This threat, self -help efforts, are almost impossible to completely remove it yourself. As explained in the lecture of Educational Module D, hackers around the world are working hard to improve their hacking techniques every day. On the other hand, vulnerabilities are latent in organizational management, and unlike threats, they can be reduced to a certain extent through self-help efforts. So what kind of self-help efforts can we take? It's very simple: it means properly complying with the security processes defined by security technical standards. Please understand that having everyone do what has been decided is directly linked to reducing vulnerability.



DEVELOPMENT SYSTEM OF SECURITY PRODUCT.

Customer

Top Management

It has the following responsibilities:
・Security development progress management
・Achieve security requirements

Product development team

Development Supervisor or Project Manager

Security leader

Responsible for carrying out all security development operations in accordance with the security plan.

Security Incident and Vulnerability response

PSIRT

Accepts, investigates, and internally coordinates product security vulnerability information.

Peer review

Technical reviewer

The role of reviewing deliverables from a professional point of expertise in security measures technology.

Audit/Assessment

Quality department

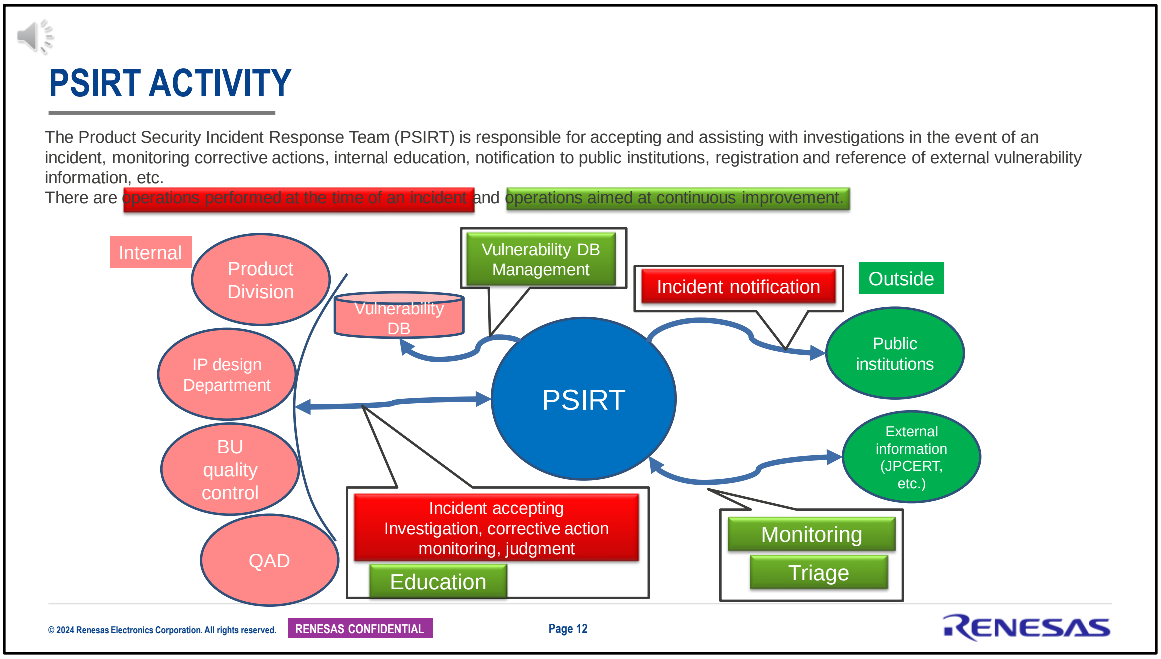
Security assessor

The role of conducting security audits and security assessments (automotive only).

In the event of a security incident vulnerability, PSIRT assists the product development team in its corrective action activities.

RENESAS CONFIDENTIAL Page 11 RENESAS

From here, we will start with a detailed explanation of JF3009. This diagram shows the security product development structure that was also explained in Module A, but today I will explain it again with an emphasis on PSIRT. By the way,the word PSIRT is used for the first time in this slide, but it is an acronym for Product Security Incident Response Team, and will be explained in more detail later. This picture shows the interactions between PSIRT and its surrounding stakeholders using arrow marks. First, the people listed in red boxes show those who are responsible for adding security value to general products and there are four roles,that is,Security leader, Technical reviewer, Security Assessor and PSIRT member. There are explanations of each roles in the speech bubble, but I will not read it out loud here Today, so please read it later by yourself. What this diagram states is that PSIRT supports product developers mainly with vulnerability information during product development, and is the backbone of activities to eliminate vulnerabilities from products through self-help efforts as explained on the previous page. From the next page, I will explain step by step how PSIRT support the development team.



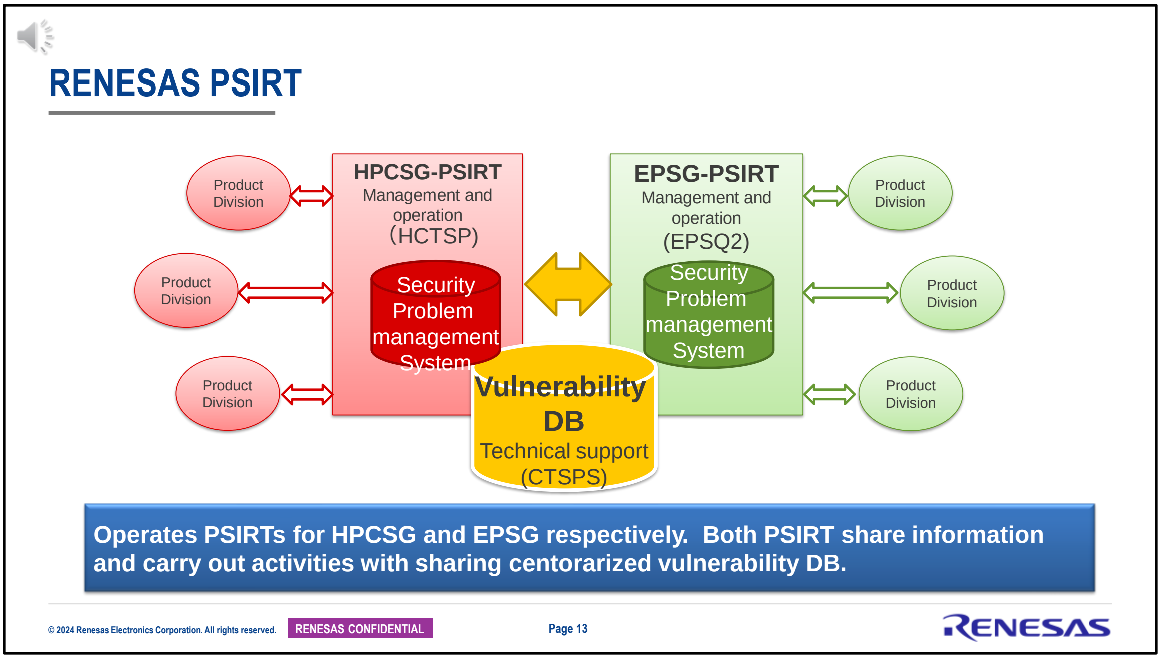
PSIRT ACTIVITY

The Product Security Incident Response Team (PSIRT) is responsible for accepting and assisting with investigations in the event of an incident, monitoring corrective actions, internal education, notification to public institutions, registration and reference of external vulnerability information, etc.
There are operations performed at the time of an incident and operations aimed at continuous improvement.

Internal
Product Division
IP design Department
BU quality control
QAD
Vulnerability DB
Vulnerability DB Management
PSIRT
Incident notification
Outside
Public institutions
External information (JPCERT, etc.)
Incident accepting Investigation, corrective action monitoring, judgment
Education
Monitoring
Triage

RENESAS CONFIDENTIAL Page 12 RENESAS

This picture shows the interactions between PSIRT and the stakeholders surrounding, and it has two pillars: firefighting activities in response to security incidents and continuous improvement activities to reduce vulnerabilities. To make it a little easier to understand, it can be said that there are activities during war and activities during peace, but in this picture, they are colored in red and green. The red square is the former activity and the green square is the latter activity. In case of an incident occurs, PSIRT receives information from the development and quality departments, supports investigations, determines measures, and then monitors, closes, and reports to public institutions. On the other hand, PSIRT carry out continuous improvement activities as a main role including update the vulnerability database used for security product development by internal and external information monitoring and information triage and conducting internal education.



RENESAS PSIRT

Product Division

Product Division

Product Division

HPCSG-PSIRT
Management and operation
(HCTSP)

Security Problem management System

EPSG-PSIRT
Management and operation
(EPSQ2)

Security Problem management System

Product Division

Product Division

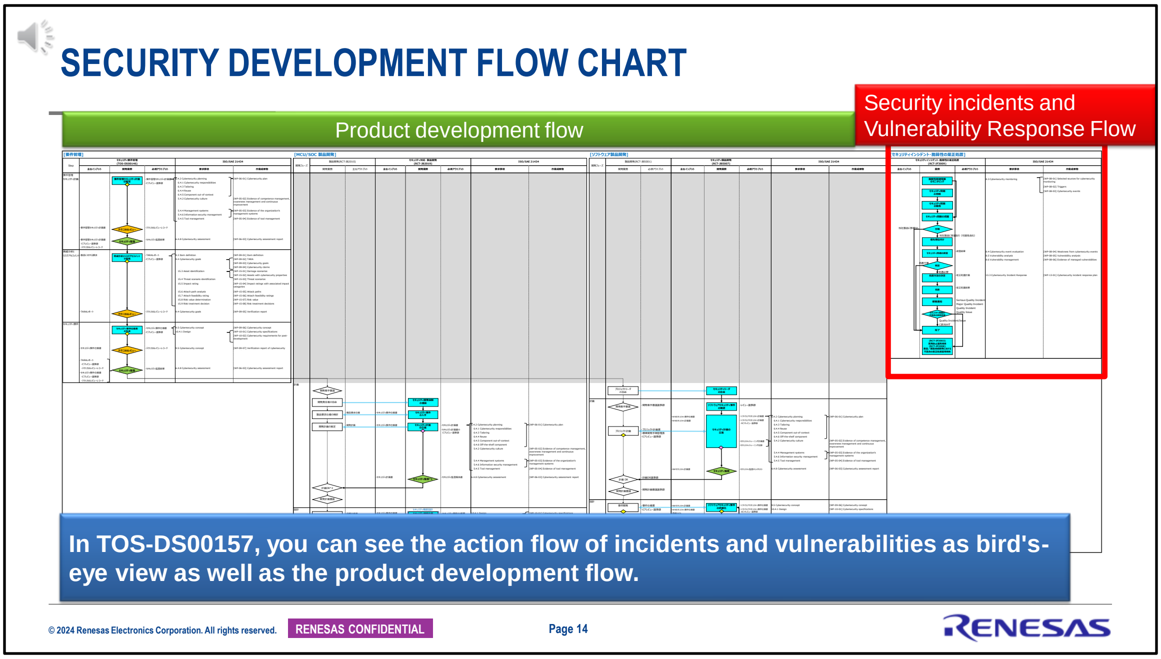
Product Division

Vulnerability DB
Technical support
(CTSPS)

Operates PSIRTs for HPCSG and EPSG respectively. Both PSIRT share information and carry out activities with sharing centorarized vulnerability DB.

RENESAS CONFIDENTIAL

This is Renesas' current PSIRT organization, which is independent of both HPCSG and EPSG. Although the systems for managing security incidents are separated, the vulnerability databases used by both PSIRT are unified as one company, and activities are carried out in coordination with each other around this center database.



SECURITY DEVELOPMENT FLOW CHART

Product development flow

Security incidents and Vulnerability Response Flow

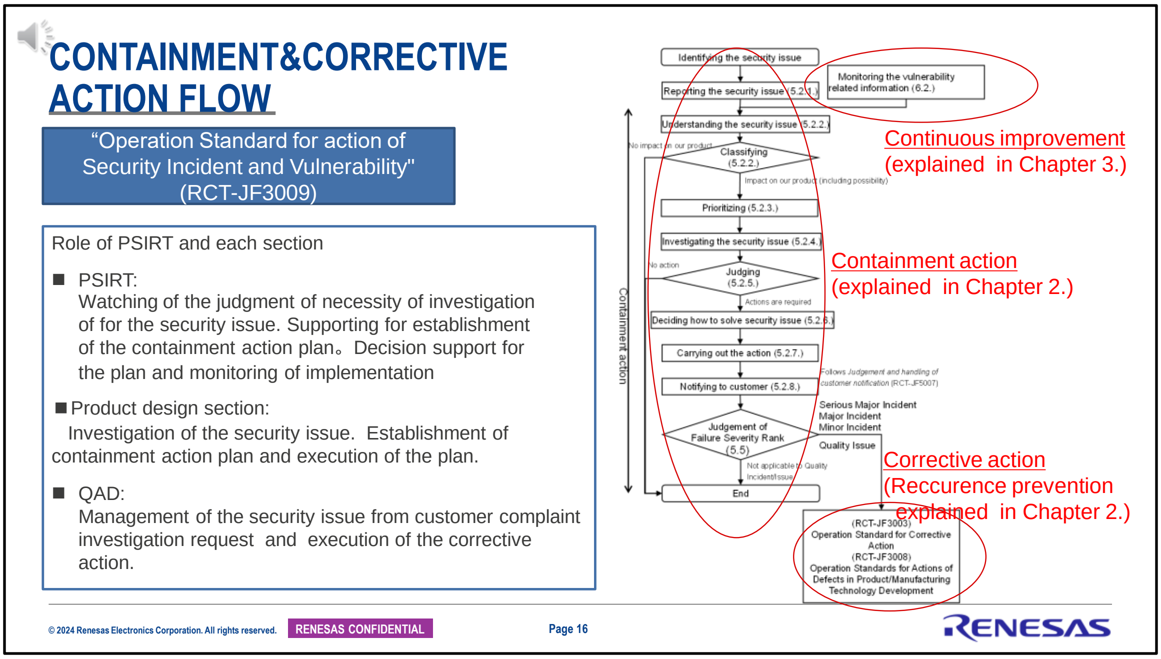
In TOS-DS00157, you can see the action flow of incidents and vulnerabilities as bird's-eye view as well as the product development flow.

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 14 RENESAS

The following figure also repeats the module A material but I explain again. This flowchart provides an overview of the incident and vulnerability treatment flow together with the product development flow. It is published in the TOS-DS00157 appendix on the Cybersecurity page of the Design Quality Portal, and anyone can view it at any time. Specifically, the part circled in red on the right side is the relevant part of this course.

2. CONTAINMENT ACTION AND CORRECTIVE ACTION FOR SECURITY ISSUES.

Chapter 2. This is a containment action and corrective action for security issues.
In Chapter 1, we explained that RCT-JF3009 defines two activities: incident response activities and continuous improvement activities, and in this Chapter 2, we will explain the details of the former.



CONTAINMENT&CORRECTIVE ACTION FLOW

"Operation Standard for action of Security Incident and Vulnerability"
(RCT-JF3009)

Role of PSIRT and each section

- ■ PSIRT:
  Watching of the judgment of necessity of investigation of for the security issue. Supporting for establishment of the containment action plan。Decision support for the plan and monitoring of implementation

■Product design section:
  Investigation of the security issue. Establishment of containment action plan and execution of the plan.

- ■ QAD:
  Management of the security issue from customer complaint investigation request and execution of the corrective action.

Identifying the security issue

Reporting the security issue (5.2.1.)

Monitoring the vulnerability related information (6.2.)

Understanding the security issue (5.2.2.)

No impact on our product

Classifying (5.2.2.)

Impact on our product (including possibility)

Prioritizing (5.2.3.)

Investigating the security issue (5.2.4.)

No action

Judging (5.2.5.)

Actions are required

Deciding how to solve security issue (5.2.6.)

Carrying out the action (5.2.7.)

Notifying to customer (5.2.8.)

Follows *Judgement and handling of customer notification* (RCT-JF5007)

Judgement of Failure Severity Rank (5.5)

Serious Major Incident
Major Incident
Minor Incident

Quality Issue

Not applicable to Quality Incident/Issue

End

Containment action

(RCT-JF3003)
Operation Standard for Corrective Action
(RCT-JF3008)
Operation Standards for Actions of Defects in Product/Manufacturing Technology Development

Continuous improvement
(explained in Chapter 3.)

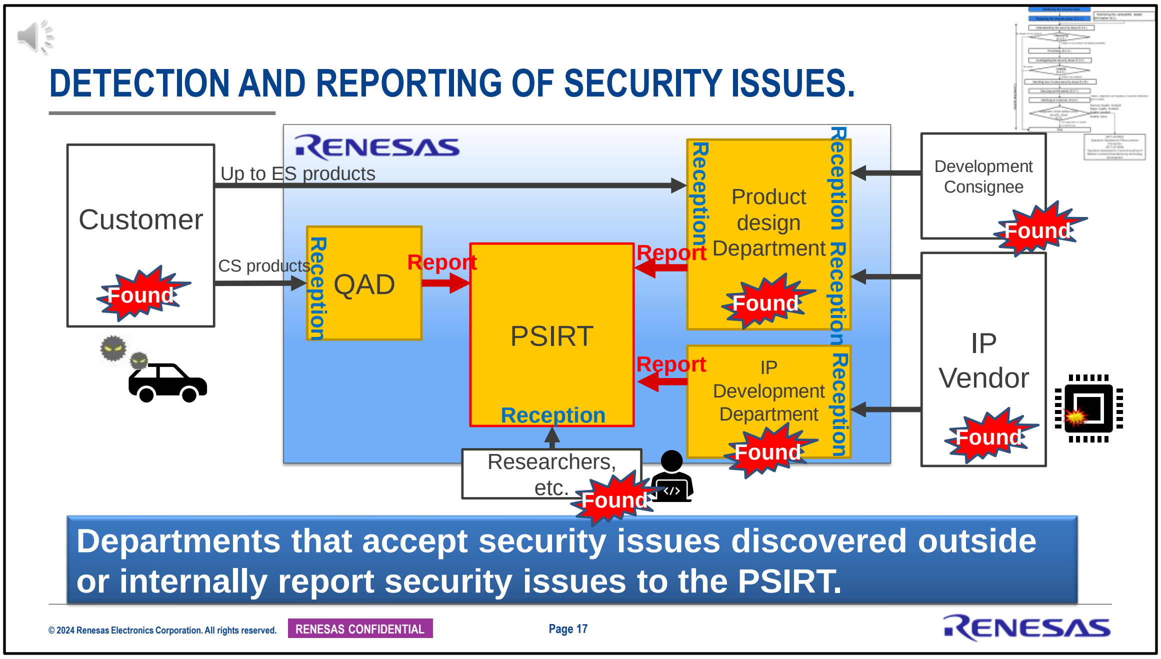
Containment action
(explained in Chapter 2.)

Corrective action
(Reccurence prevention explained in Chapter 2.)

RENESAS CONFIDENTIAL

Page 16

This slide is the security issues containment action flow shown in RCT-JF3009. The area circled in red in the upper right corner represents the input from continuous improvement activities by vulnerability information monitoring both inside and outside of Renesas, which will be explained in Chapter 3 later. This flow covers everything from detection of security issues to completion of containment action and recurrence prevention,but everything written here is not done by PSIRT members only. As you can see in the box on the left, PSIRT,Design department and Quality assurance department share their responsible job steps. I will explain the details in following pages.



DETECTION AND REPORTING OF SECURITY ISSUES.

RENESAS

Customer

Found

Up to ES products

CS products

Reception

QAD

Report

PSIRT

Reception

Reception

Product design Department

Reception

Found

Report

IP Development Department

Reception

Found

Development Consignee

Found

IP Vendor

Found

Researchers, etc.

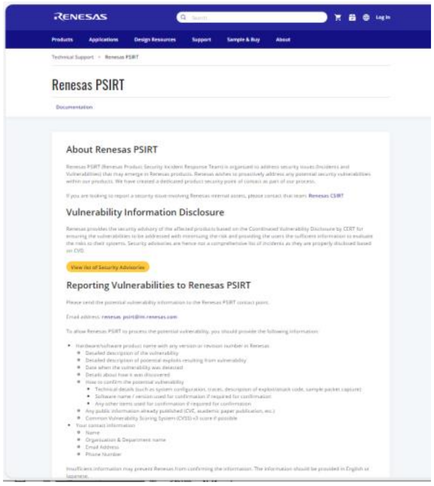
Found

Departments that accept security issues discovered outside or internally report security issues to the PSIRT.

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 17 RENESAS

First, I will explain the flow of reporting to PSIRT from the detection of security issues. This will be common to subsequent pages in this chapter, but I have pasted a small picture of the security issues processing flow in the upper right corner, and have indicated the relevant steps explained in the page in blue, so you can reconfirm the relevant steps on each page. The diagram on this slide is an extension of the diagram on page 11 to include external customers, development contractors, and IP vendors. We have added an explosion mark to the scene where an incident was detected and
a reception mark to the Renesas contact point to help people understand the flow of information being ultimately aggregated to PSIRT. As you can see, each person who receives information about security issues detected outside of Renesas becomes the person requesting the investigation, and the security issues are ultimately reported to PSIRT.

RENESAS PSIRT ANNOUNCED TO THE OUTSIDE.



Renesas PSIRT

Documentation

About Renesas PSIRT

Renesas PSIRT (Renesas Product Security Incident Response Team) is organized to address security issues (Incidents and Vulnerabilities) that may emerge in Renesas products. Renesas wishes to proactively address any potential security vulnerabilities within our products. We have created a dedicated product security point of contact as part of our process.

If you are looking to report a security issue involving Renesas internal assets, please contact that team: Renesas CSIRT

Vulnerability Information Disclosure

Renesas provides the security advisory of the affected products based on the Coordinated Vulnerability Disclosure by CERT for ensuring the vulnerabilities to be addressed with minimizing the risk and providing the users the sufficient information to evaluate the risks to their systems. Security advisories are hence not a comprehensive list of incidents as they are properly disclosed based on CVD.

View list of Security Advisories

Reporting Vulnerabilities to Renesas PSIRT

Please send the potential vulnerability information to the Renesas PSIRT contact point.

Email address: renesas_psirt@lm.renesas.com

To allow Renesas PSIRT to process the potential vulnerability, you should provide the following information:

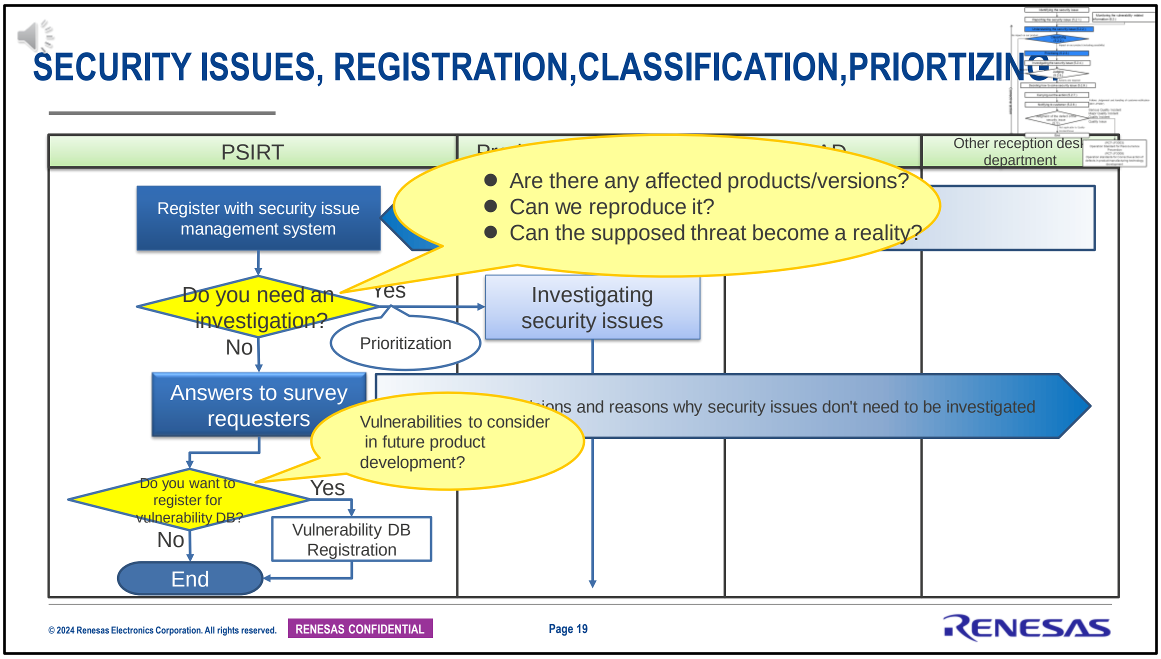
- Hardware/software product name with any version or revision number in Renesas
  - Detailed description of the vulnerability
  - Detailed description of potential exploits resulting from vulnerability
  - Date when the vulnerability was detected
  - Details about how it was discovered
  - How to confirm the potential vulnerability
    - Technical details (such as system configuration, traces, description of exploit/attack code, sample packet capture)
    - Software name / version used for confirmation if required for confirmation
    - Any other items used for confirmation if required for confirmation
  - Any public information already published (CVE, academic paper publication, etc.)
  - Common Vulnerability Scoring System (CVSS) v3 score if possible
- Your contact information
  - Name
  - Organisation & Department name
  - Email Address
  - Phone Number

Insufficient information may prevent Renesas from confirming the information. The information should be provided in English or Japanese.

https://www.renesas.com/jp/ja/support/renesas-psirt.html

RENESAS CONFIDENTIAL

This is a snapshot image of the PSIRT counter established on the Renesas external web portal as a point of contact for receiving information on security issues from outside Renesas. However, as explained on the previous page, security issues information is not only received through this portal, but also when it is received as a normal customer complaint, or when it is sent to the design department via sales for individual technical consultation, or when it is sent from a research institution to the PSIRT department. In some cases, external information is received directly, and there are actually various sources of external information.



SECURITY ISSUES, REGISTRATION,CLASSIFICATION,PRIORTIZING

PSIRT

Other reception desk department

Register with security issue management system

- Are there any affected products/versions?
- Can we reproduce it?
- Can the supposed threat become a reality?

Do you need an investigation?

Yes

No

Prioritization

Investigating security issues

Answers to survey requesters

ions and reasons why security issues don't need to be investigated

Vulnerabilities to consider in future product development?

Do you want to register for vulnerability DB?

Yes

No

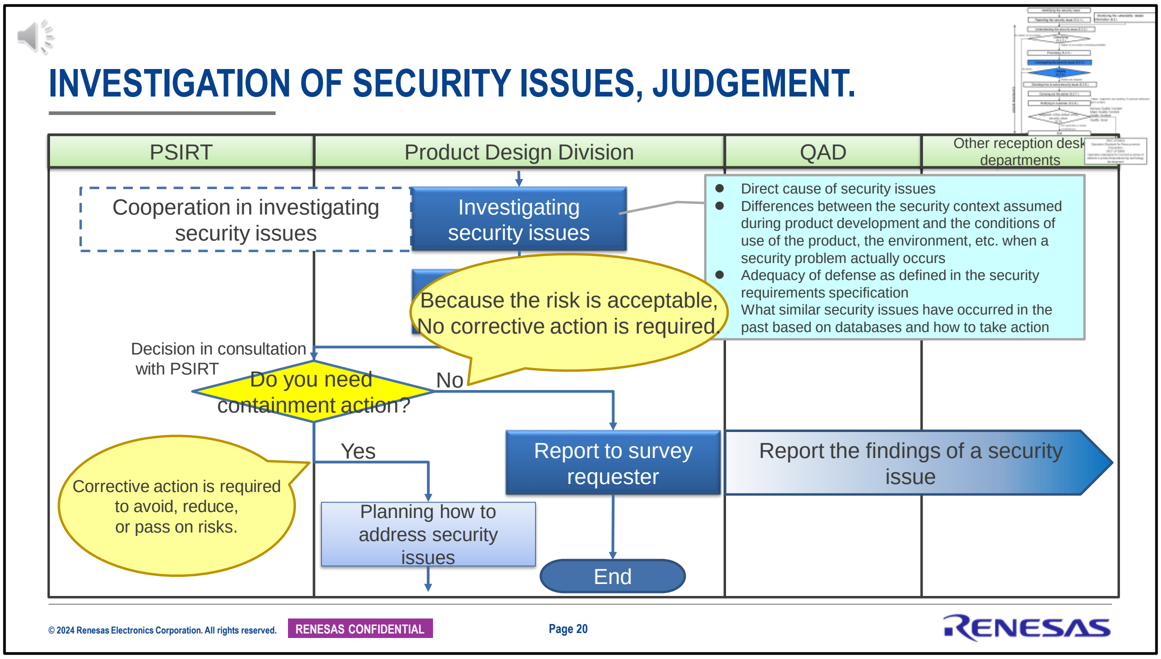
Vulnerability DB Registration

End

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL

Page 19

Next, we will explain the steps taken by PSIRT, that is, registration, classification, and prioritizing security issues after receiving a report from each security issues investigation requester. First, PSIRT member registers the information in the security issues management system explained on page 13, and then assesses whether a detailed investigation is really necessary or not . As stated in the large speech bubble at the top of slide, the criteria used for assessment is whether the issues affect Renesas products or not, whether the issues can be reproductive, and whether the threat supposed by the issues is realistic. And If it is determined that investigation is necessary, we will proceed to the investigation process from the next page, but if it is determined that it is not necessary investigation, we will respond to the investigation requester with the reason why the investigation is not necessary and will decide whether registration to the vulnerability database is necessary or not for future product development. If it is determined the information is valuable enough, we will register it in the vulnerability database and complete this series action.



INVESTIGATION OF SECURITY ISSUES, JUDGEMENT.

PSIRT

Product Design Division

QAD

Other reception desk departments

Cooperation in investigating security issues

Investigating security issues

- Direct cause of security issues
- Differences between the security context assumed during product development and the conditions of use of the product, the environment, etc. when a security problem actually occurs
- Adequacy of defense as defined in the security requirements specification
  What similar security issues have occurred in the past based on databases and how to take action

Because the risk is acceptable, No corrective action is required

Decision in consultation with PSIRT

Do you need containment action?

No

Yes

Corrective action is required to avoid, reduce, or pass on risks.

Report to survey requester

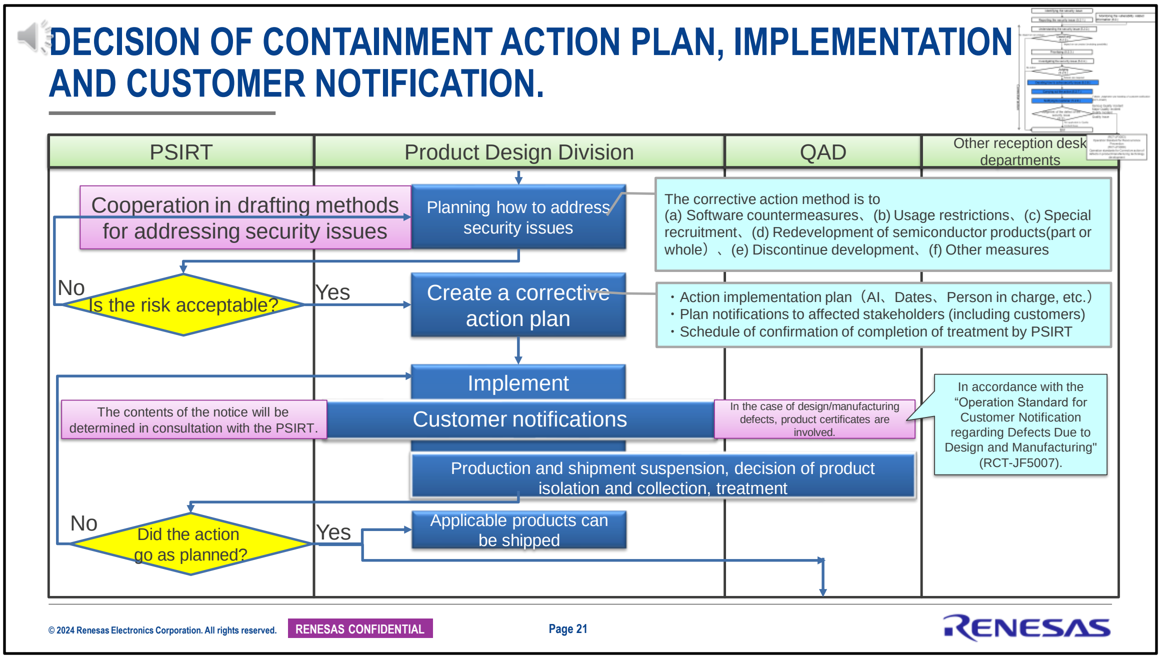
Report the findings of a security issue

Planning how to address security issues

End

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 20

Next, we will explain the steps for investigating and judgement of security issues. This is the flow followed by the previous page that in case of investigation is necessary. Security issues will be investigated by the design department with the support of PSIRT and security risks will be estimated based on the investigation results. As shown in the blue square bubble in the upper right corner,what we are investigating is not only the cause, but also the usage conditions of the product that were assumed at the time of development and also the usage conditions when the problem actually occurred. Is there any difference? Were the security defense measures defined in the security requirements specification created at the time of development sufficient? Were countermeasures for similar problems already implemented in the vulnerability database at the time of development? Etc. In short,the first thing to do is to check whether the established security development process properly followed or not at the time of development of affected product. Based on the results, the necessity of containment action will be determined based on the estimated risk. If action is required,proceed to the flow on the next page.



DECISION OF CONTAINMENT ACTION PLAN, IMPLEMENTATION AND CUSTOMER NOTIFICATION.

PSIRT	Product Design Division	QAD	Other reception desk departments

Cooperation in drafting methods for addressing security issues

Planning how to address security issues

The corrective action method is to
(a) Software countermeasures、(b) Usage restrictions、(c) Special recruitment、(d) Redevelopment of semiconductor products(part or whole）、(e) Discontinue development、(f) Other measures

Is the risk acceptable?

No

Yes

Create a corrective action plan

・Action implementation plan（AI、Dates、Person in charge, etc.）
・Plan notifications to affected stakeholders (including customers)
・Schedule of confirmation of completion of treatment by PSIRT

Implement

The contents of the notice will be determined in consultation with the PSIRT.

Customer notifications

In the case of design/manufacturing defects, product certificates are involved.

In accordance with the "Operation Standard for Customer Notification regarding Defects Due to Design and Manufacturing" (RCT-JF5007).

Production and shipment suspension, decision of product isolation and collection, treatment

Did the action go as planned?

No

Yes

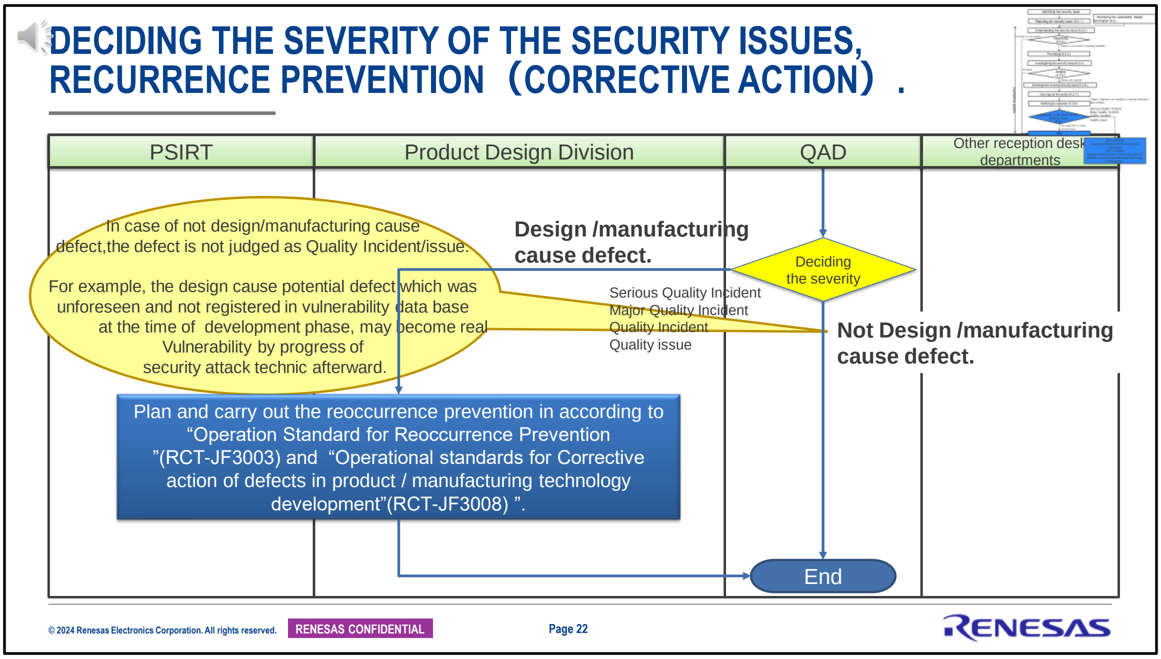
Applicable products can be shipped

RENESAS CONFIDENTIAL

Page 21

RENESAS

Next,we will explain handling security issues, so that how to decide action plan, action implementation and notification for customers. Based on the risk estimated in the previous flow, the design department plan the containment action and PSIRT determines that the resulted reduction risk after action is within an acceptable range. If the reduction risk is within an acceptable range, the containment action plan will be documented and the design department will take the lead in implementing the plan, notifying customers, and handling the product in cooperation with related departments.



DECIDING THE SEVERITY OF THE SECURITY ISSUES, RECURRENCE PREVENTION （CORRECTIVE ACTION） .

PSIRT	Product Design Division	QAD	Other reception desk departments

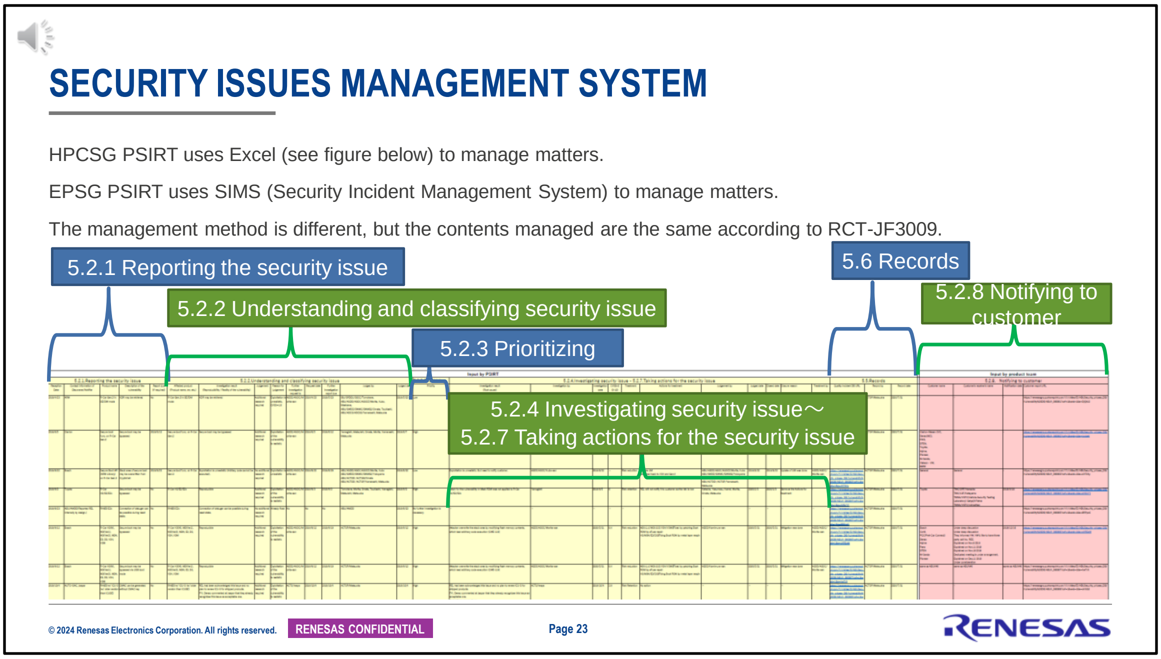
In case of not design/manufacturing cause defect,the defect is not judged as Quality Incident/issue.

For example, the design cause potential defect which was unforeseen and not registered in vulnerability data base at the time of development phase, may become real Vulnerability by progress of security attack technic afterward.

Plan and carry out the reoccurrence prevention in according to “Operation Standard for Reoccurrence Prevention ”(RCT-JF3003) and “Operational standards for Corrective action of defects in product / manufacturing technology development”(RCT-JF3008) ”.

RENESAS CONFIDENTIAL Page 22

Next, we will explain how to determine the severity of security issues and prevent recurrence.　Followed by the previous flow, Quality control department determines whether it is design /manufacturing related defect or not for which Renesas is responsible. If it is judged as design/manufacturing related defect, the design department classifies the defect based on RCT-JF3003 and 3008 and plan and implement measures to prevent recurrence, and completes the incident handling flow.　On the other hand, the cases where it is not considered to be a design/manufacturing defect that was caused by not registered as vulnerability case in the vulnerability database at the time of development but later became a vulnerability due to updating of hacker technology, as shown in the yellow speech bubble.
In other words, it is essential to check the history of the vulnerability database used during development to determine whether the defect is the fault of Renesas' responsible or not.



SECURITY ISSUES MANAGEMENT SYSTEM

HPCSG PSIRT uses Excel (see figure below) to manage matters.

EPSG PSIRT uses SIMS (Security Incident Management System) to manage matters.

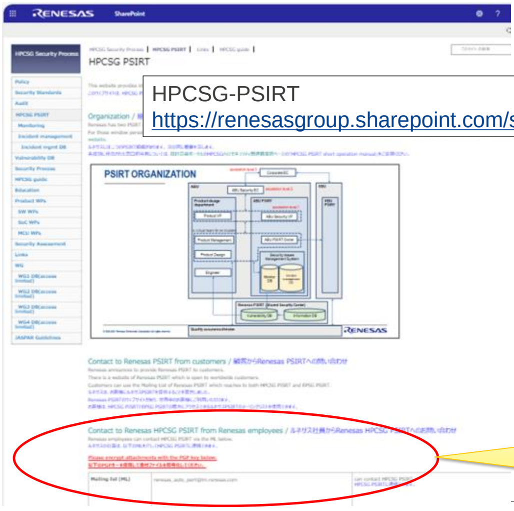
The management method is different, but the contents managed are the same according to RCT-JF3009.

5.2.1 Reporting the security issue
5.2.2 Understanding and classifying security issue
5.2.3 Prioritizing
5.2.4 Investigating security issue～
5.2.7 Taking actions for the security issue
5.6 Records
5.2.8 Notifying to customer
Input by PSIRT
Input by product team
5.2.1.Reporting the security issue
5.2.2.Understanding and classifying security issue

RENESAS CONFIDENTIAL

This concludes the explanation of the incident flow, but I would like to introduce an example of the security issues management system that came up during former explanation. This is an example of Excel sheet used by HPCSG PSIRT, and basically the format is to record the information output at each steps of the flow explained earlier.

HOW TO CONTACT HPCSG-PSIRT



HPCSG PSIRT

PSIRT ORGANIZATION

Contact to Renesas PSIRT from customers / 顧客からRenesas PSIRTへの問い合わせ

Contact to Renesas HPCSG PSIRT from Renesas employees / ルネサス社員からRenesas HPCSG PSIRTへのお問い合わせ

Please encrypt attachments with the PGP key below.

Mailing list (ML)	renesas_auto_psirt@lm.renesas.com

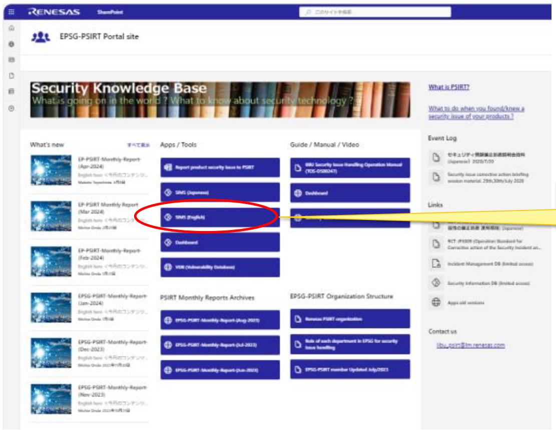
HPCSG-PSIRT
https://renesasgroup.sharepoint.com/sites/EI/ABUSecurity_oricess_DB/Pages/ABU-PSIRT.aspx

HPCSG-PSIRT
mailing list.

RENESAS CONFIDENTIAL

This is WEB page that describes how to report security issues to HPCSG-PSIRT. Please click on the URL below to check later.

HOW TO CONTACT EPSG-PSIRT

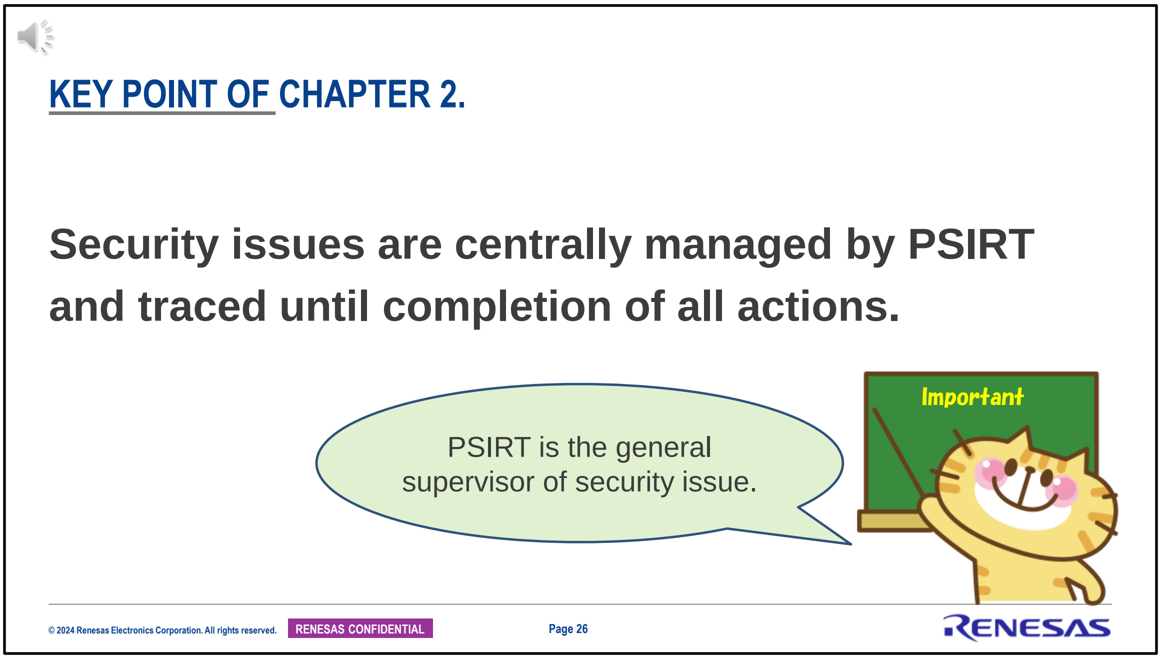

RENESAS SharePoint
EPSG-PSIRT Portal site
Security Knowledge Base
What is going on in the world ? What to know about security technology ?
What's new
EP-PSIRT-Monthly-Report (Apr-2024)
EP-PSIRT Monthly Report (Mar 2024)
EP-PSIRT-Monthly-Report (Feb-2024)
EPSG-PSIRT-Monthly-Report (Jan-2024)
EPSG-PSIRT-Monthly-Report (Dec-2023)
EPSG-PSIRT-Monthly-Report (Nov-2023)
Apps / Tools
Report product security issue to PSIRT
SIMS (Japanese)
SIMS (English)
Dashboard
VDB (Vulnerability Database)
PSIRT Monthly Reports Archives
EPSG-PSIRT-Monthly-Report-(Aug-2023)
EPSG-PSIRT-Monthly-Report-(Jul-2023)
EPSG-PSIRT-Monthly-Report-(Jun-2023)
Guide / Manual / Video
IBU Security Issue Handling Operation Manual (TDS-DS00347)
Dashboard
EPSG-PSIRT Organization Structure
Renesas PSIRT organization
Role of each department in EPSG for security issue handling
EPSG-PSIRT member Updated July2023
What is PSIRT?
What to do when you found/knew a security issue of your products ?
Event Log
Security issue corrective action briefing session material. 29th,30th/July 2020
Links
Incident Management DB (limited access)
Security Information DB (limited access)
Apps old versions
Contact us
ibu_psirt@lm.renesas.com

Security Issue Management System (SIMS).

EPSG-PSIRT EPSG-PSIRT Portal site - Home (sharepoint.com)

RENESAS CONFIDENTIAL

Meanwhile, here is the page that describes how to report security issues to EPSG-PSIRT. The content of incident management is almost the same as HPCSG, but here we operate a system so called SIMS. Please click on the URL below and check it later.



KEY POINT OF CHAPTER 2.

Security issues are centrally managed by PSIRT and traced until completion of all actions.

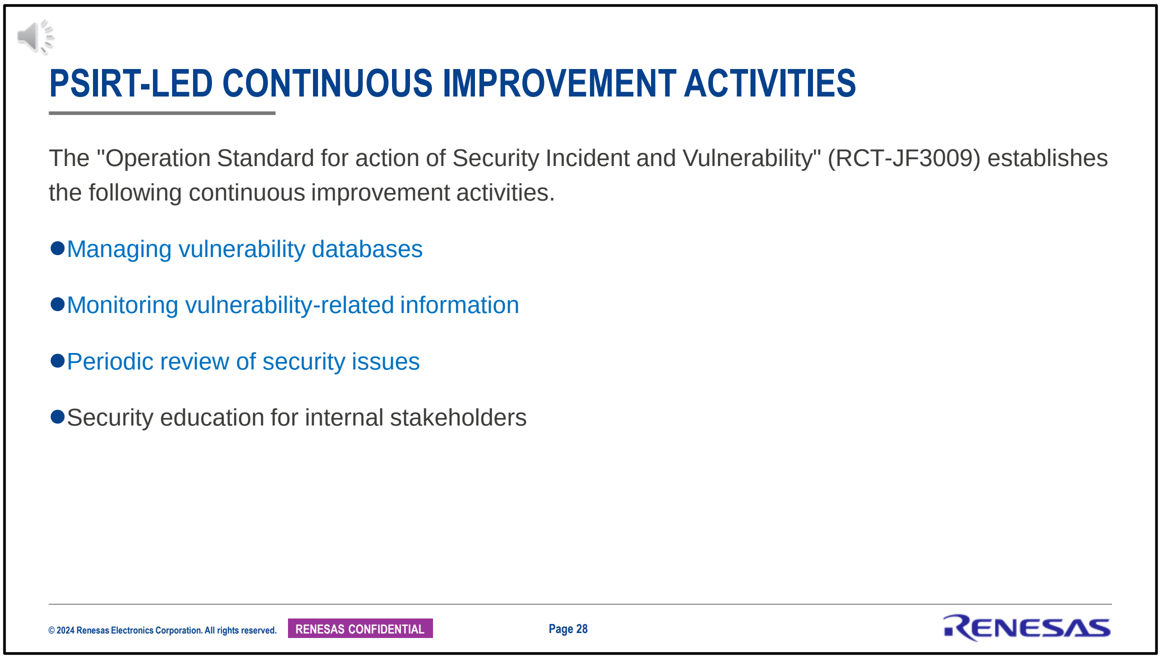
PSIRT is the general supervisor of security issue.

RENESAS CONFIDENTIAL

This is the end of Chapter 2.
Briefly summarize the main points, although PSIRT does not handle security issue alone but is responsible for the unified management of information and tracing until resolution is completed.
So it can be said that PSIRT is “general supervisor of security”.

3. CONTINUOUS IMPROVEMENT ACTIVITIES

Chapter 3. This is a continuous improvement activity.
In Chapter 1, we explained that RCT-JF3009 defines two activities: incident response activities and continuous improvement activities, and in this Chapter 3, we will continue to explain the details of the latter.



PSIRT-LED CONTINUOUS IMPROVEMENT ACTIVITIES

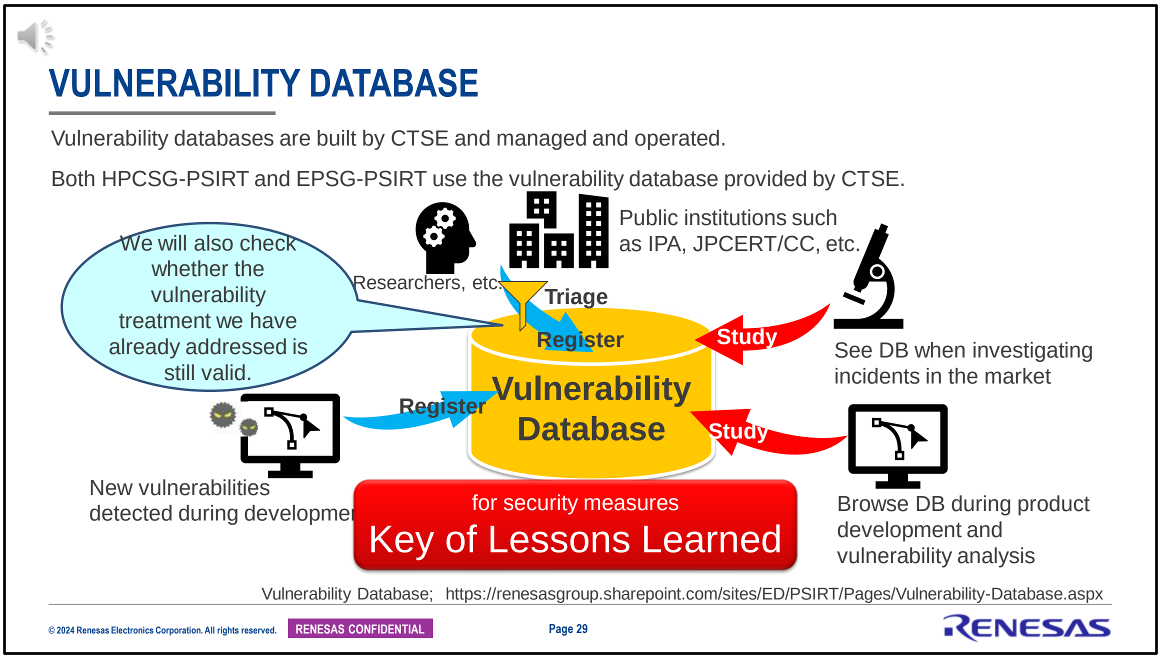
The "Operation Standard for action of Security Incident and Vulnerability" (RCT-JF3009) establishes the following continuous improvement activities.

- ●Managing vulnerability databases
- ●Monitoring vulnerability-related information
- ●Periodic review of security issues
- ●Security education for internal stakeholders

RENESAS CONFIDENTIAL

Page 28

There are four activities that PSIRT carries out as continuous improvement activities shown here, but in this chapter 3,
we will explain three of them, which are in blue: managing the vulnerability database, monitoring vulnerability information, and periodic review of security issues.



VULNERABILITY DATABASE

Vulnerability databases are built by CTSE and managed and operated.

Both HPCSG-PSIRT and EPSG-PSIRT use the vulnerability database provided by CTSE.

We will also check whether the vulnerability treatment we have already addressed is still valid.

Researchers, etc.
Public institutions such as IPA, JPCERT/CC, etc.
Triage
Register
Study
See DB when investigating incidents in the market
Register
Vulnerability Database
Study
New vulnerabilities detected during developmen
Browse DB during product development and vulnerability analysis

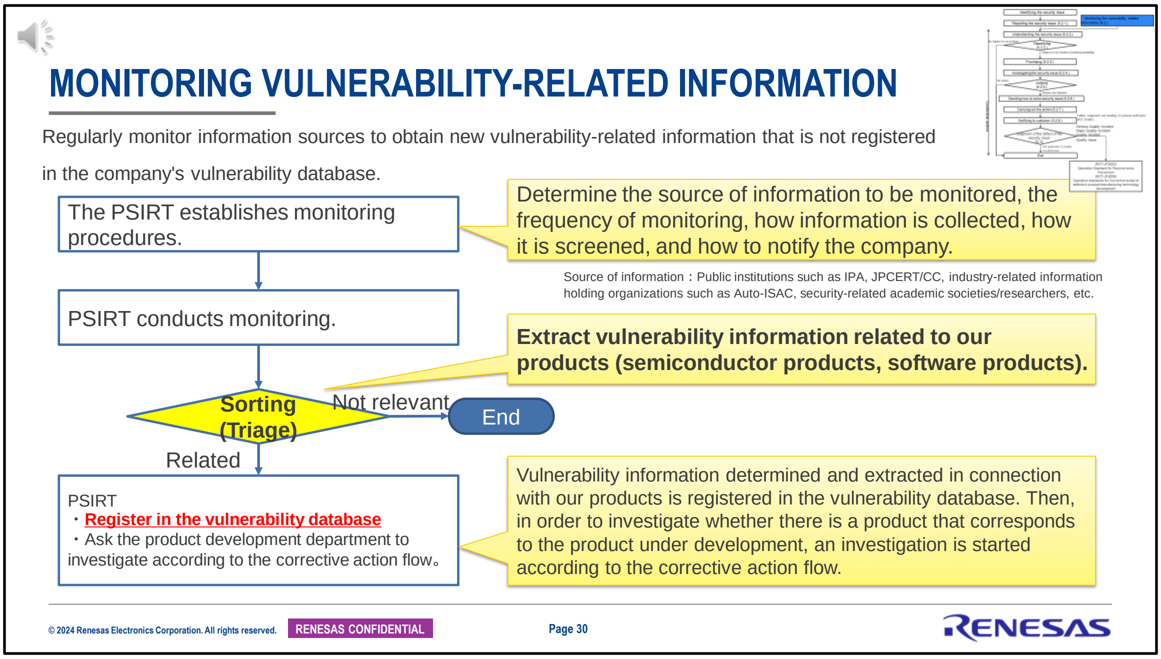
for security measures

Key of Lessons Learned

Vulnerability Database; https://renesasgroup.sharepoint.com/sites/ED/PSIRT/Pages/Vulnerability-Database.aspx

RENESAS CONFIDENTIAL Page 29 RENESAS

First, let‘s talk about vulnerability database management. As mentioned in Chapter 1, the vulnerability database is constructed and managed by CTSPS as a company-wide database, and is used by HPCSG and EPSG designers and PSIRT members for product development, incident management, etc. In this diagram, blue arrows indicate which information sources the vulnerability information comes from, and red arrows indicate how that information is used within the company. Blue is input and red is output, so as you can see, the vulnerability database is the key to security management. There are two types of input: input comes from external sources such as public institutions and researchers, and input comes from within Renesas, such as newly detected items during the development process of new products. On the other hand, there are two types of output: one is used for incident response investigation, and the other is used for vulnerability analysis in product development. Naturally, if this database information were leaked outside the company, it could be misused by hackers and cause serious problems, so it is managed at an extremely higher security level and strict disclosure restrictions are in place. This means that not everyone can see it. The term security level has now been mentioned, but this is specified in RCT-JB0026 and explained in Process Basic Education Module D, so please refer to it.



MONITORING VULNERABILITY-RELATED INFORMATION

Regularly monitor information sources to obtain new vulnerability-related information that is not registered in the company's vulnerability database.

The PSIRT establishes monitoring procedures.

Determine the source of information to be monitored, the frequency of monitoring, how information is collected, how it is screened, and how to notify the company.

Source of information：Public institutions such as IPA, JPCERT/CC, industry-related information holding organizations such as Auto-ISAC, security-related academic societies/researchers, etc.

PSIRT conducts monitoring.

Extract vulnerability information related to our products (semiconductor products, software products).

PSIRT
・**Register in the vulnerability database**
・Ask the product development department to investigate according to the corrective action flow。

Vulnerability information determined and extracted in connection with our products is registered in the vulnerability database. Then, in order to investigate whether there is a product that corresponds to the product under development, an investigation is started according to the corrective action flow.

RENESAS CONFIDENTIAL

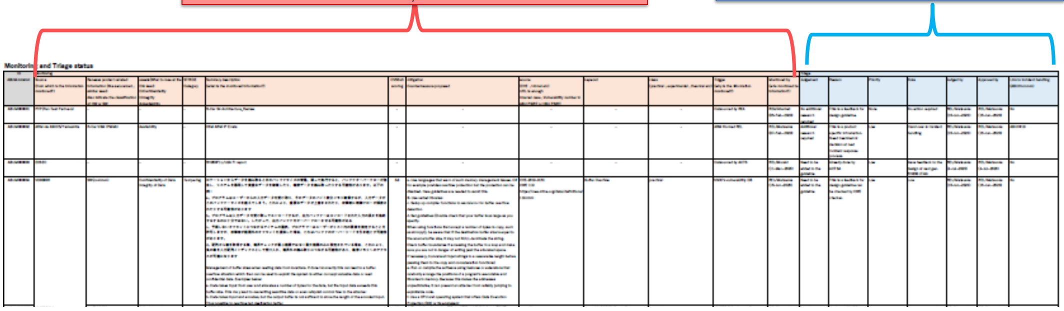
Next, I will explain the second method, vulnerability information monitoring. First of all, PSIRT establishes monitoring procedures. As shown in the yellow speech bubble on the right, this step includes specific public agency information sources, how often they should be researched, and how to collect, select, and disseminate information externally. Once these procedures are decided, regular monitoring of internal and external vulnerability information is carried out in accordance with these procedures, and the database is managed to maintain it at a world standard level.

However, bringing in any all external information would result in a huge database, so the database is registered after performing triage, which narrows down the information to only vulnerabilities related to Renesas products.

EXAMPLES OF VULNERABILITY-RELATED INFORMATION MONITORING

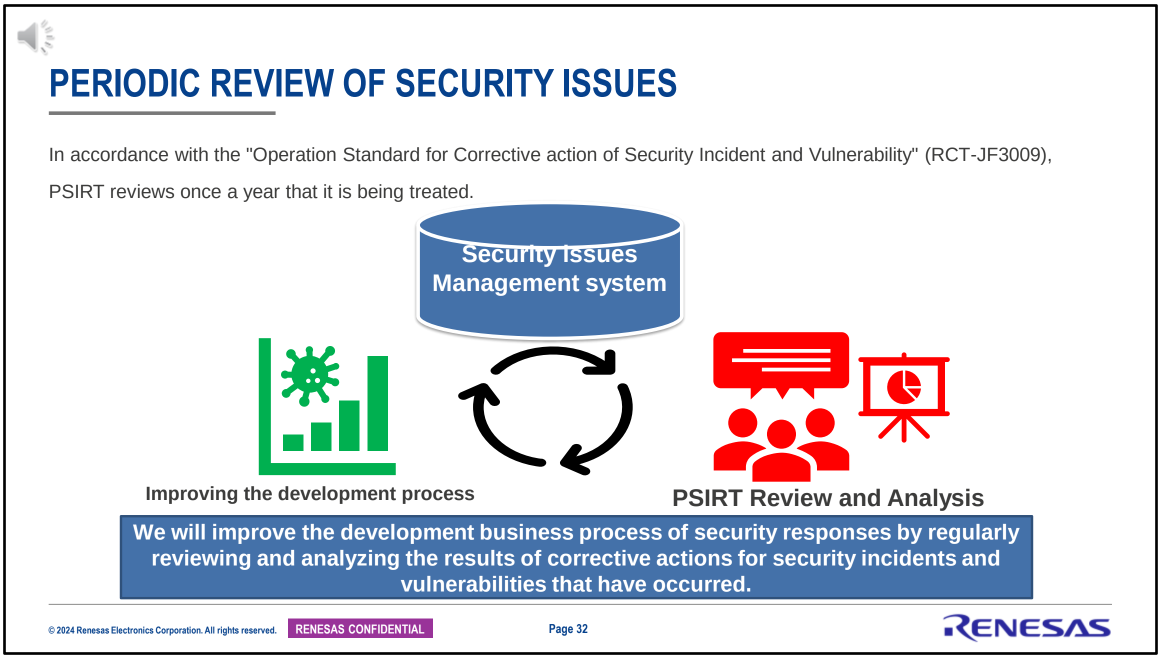
Record vulnerability information obtained by monitoring
・Information source
・Related Our Products
・CVSS risk estimates, etc.

Record treatment results
・Results and reasons for determining whether or not treatment is required
・Management IDs on security issue management systems, etc.



Monitoring and Triage status

The monitoring information I just explained is managed in a table like this as a vulnerability database. This red column is the source of vulnerability information, and includes the name of the related Renesas product and the results of risk estimation. The blue column will contain the details of the actions taken within the company and the ID management number used to link it to the security issues management system explained in Chapter 2.



PERIODIC REVIEW OF SECURITY ISSUES

In accordance with the "Operation Standard for Corrective action of Security Incident and Vulnerability" (RCT-JF3009), PSIRT reviews once a year that it is being treated.

Security Issues Management system

Improving the development process

PSIRT Review and Analysis

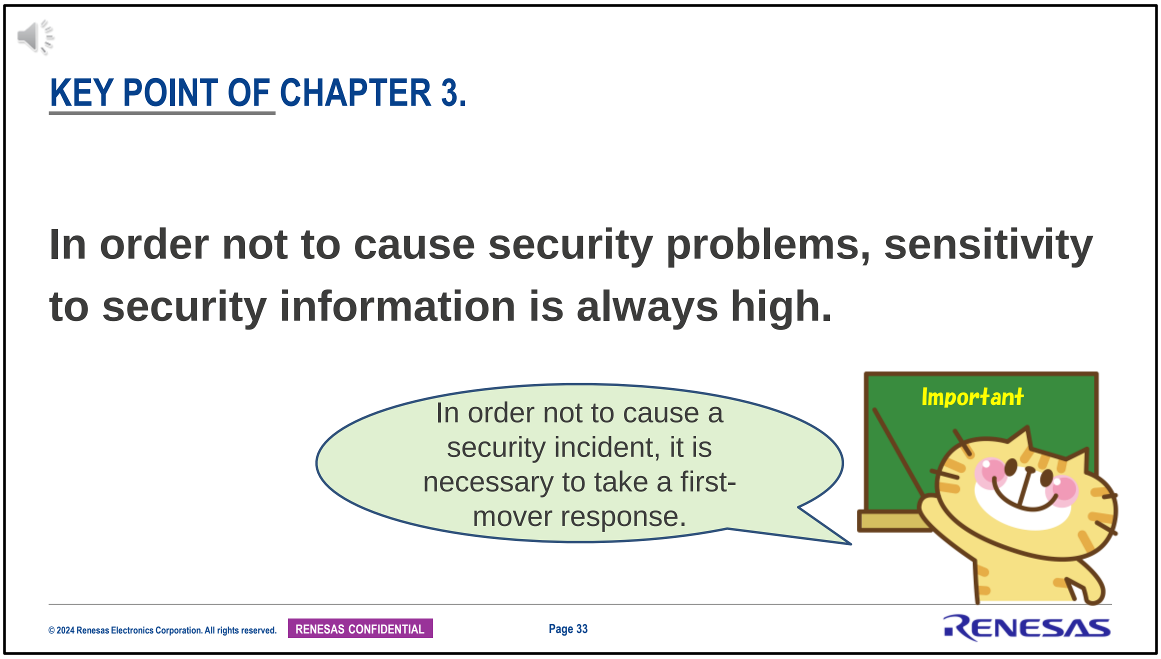
We will improve the development business process of security responses by regularly reviewing and analyzing the results of corrective actions for security incidents and vulnerabilities that have occurred.

RENESAS CONFIDENTIAL

Page 32

RENESAS

Finally, let's talk about the third part, periodic reviews of security issues. Once a year, we review whether the containment and corrective action activities in the event of security issues as explained in Chapter 2 and the periodic monitoring explained in this chapter are actually being implemented or not, in accordance with the rules of RCT-JF3009. This review is about PSIRT process. The purpose is to improve business processes based on the audit of PSIRT process,so the audit purpose is different from security assessment to judge the compliance of developed product regarding ISO21434 requirements.



KEY POINT OF CHAPTER 3.

In order not to cause security problems, sensitivity to security information is always high.

In order not to cause a security incident, it is necessary to take a first-mover response.

RENESAS CONFIDENTIAL

RENESAS

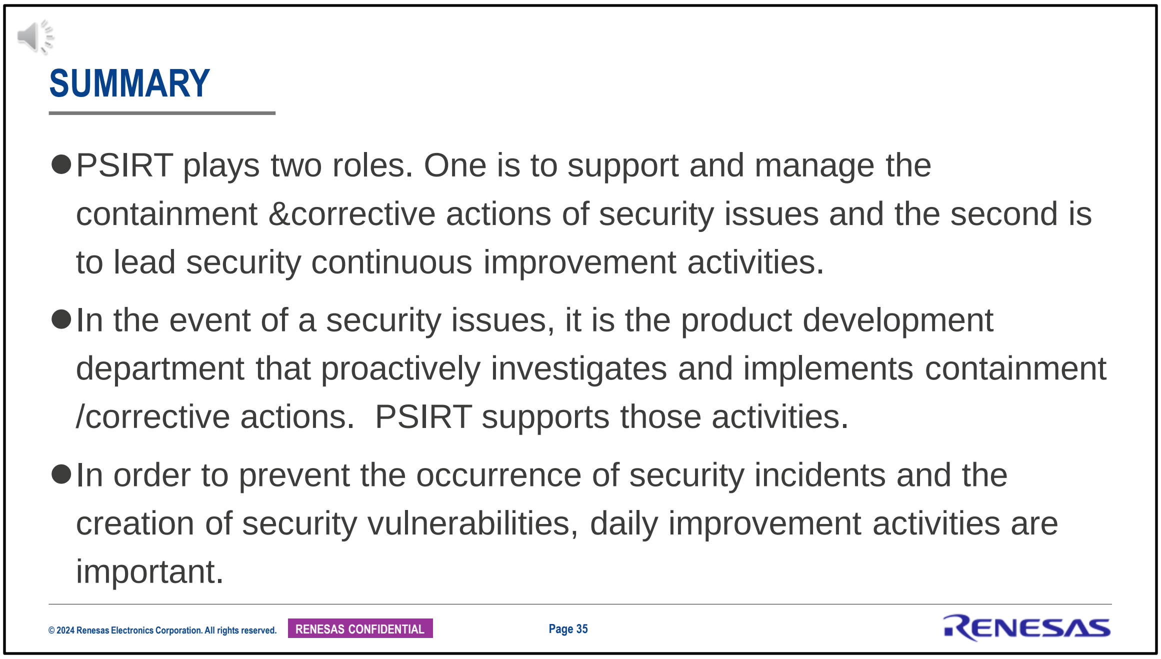
This concludes the explanation of continuous improvement activities in Chapter 3, but the key point is to increase sensitivity to security information on a daily basis in order to prevent security problems from occurring. In other words, increasing sensitivity means constantly increasing the awareness of vulnerability information both inside and outside the company and keeping the vulnerability database fresh. Furthermore, even if you only raise the antenna height or update the database, it will be completely meaningless if you neglect to deal with known vulnerabilities on a daily basis. It is important to both keep your antennae high and continue to respond appropriately to the information you receive. This is not PSIRT only limited job but job for all stakeholders.

4. SUMMARY

RENESAS CONFIDENTIAL

RENESAS

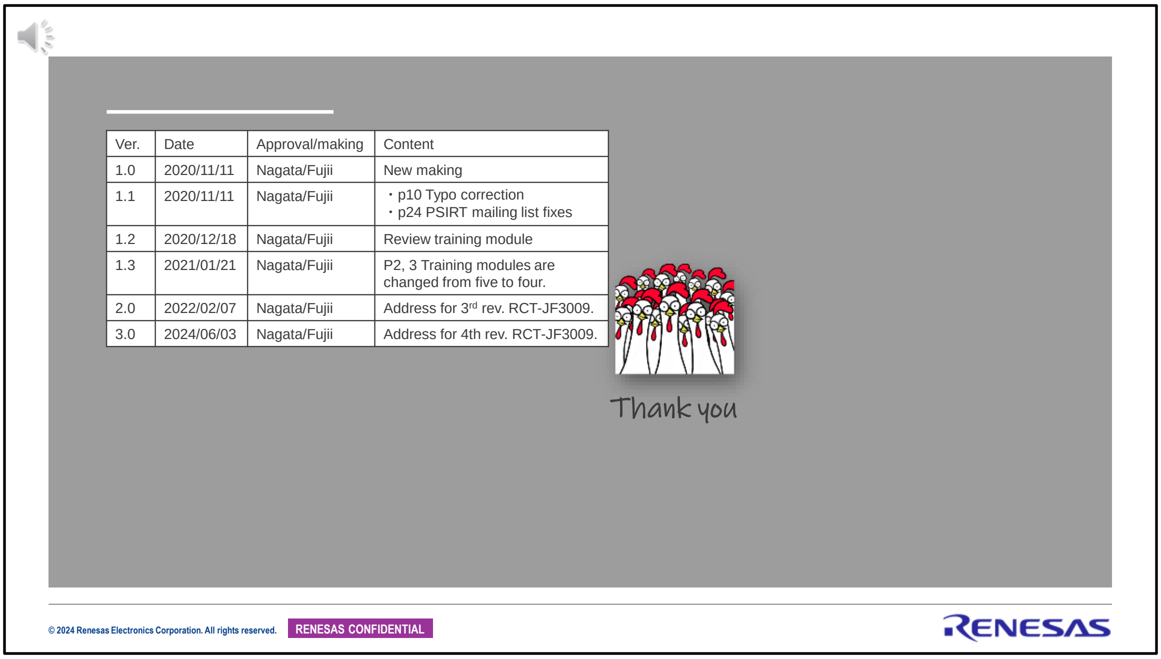
This is the final summary of this course.



SUMMARY

- PSIRT plays two roles. One is to support and manage the containment &corrective actions of security issues and the second is to lead security continuous improvement activities.
- In the event of a security issues, it is the product development department that proactively investigates and implements containment /corrective actions. PSIRT supports those activities.
- In order to prevent the occurrence of security incidents and the creation of security vulnerabilities, daily improvement activities are important.

I have explained chapters 1 to 3 so far and I briefly summarize the whole thing with these three points. Please read this on your own and use it for necessary review and daily work.
This course is a summary of the essence of RCT-JF3009.
What is your impression?
Above all, please be sure to read this RCT-JF3009 once from top to bottom to solidify your understanding.
Now this concludes Module C course, but if you are required certification on certain security role, you will need proof that you have completed this training.
This course includes simple comprehension quiz in web page,
so please take the test in succession and keep and use the comprehension test pass and a snapshot of the screen displayed as proof of attendance evidence.
Thank you for your kind listening.



Ver.	Date	Approval/making	Content
1.0	2020/11/11	Nagata/Fujii	New making
1.1	2020/11/11	Nagata/Fujii	・p10 Typo correction ・p24 PSIRT mailing list fixes
1.2	2020/12/18	Nagata/Fujii	Review training module
1.3	2021/01/21	Nagata/Fujii	P2, 3 Training modules are changed from five to four.
2.0	2022/02/07	Nagata/Fujii	Address for 3rd rev. RCT-JF3009.
3.0	2024/06/03	Nagata/Fujii	Address for 4th rev. RCT-JF3009.

Thank you

RENESAS CONFIDENTIAL